SPOTLIGHT

Sponsored by: Juniper Networks

Organizations are increasingly looking to apply AI-enhanced management to the full stack of their network, including for SD-WAN. IDC survey data shows that doing so can enable a range of benefits from increased staff productivity and enhanced security to operational efficiency and improved end-user experiences.

Enhancing Network Efficiency and Security: Integrating SD-WAN and AIOps with a Full-Stack Platform

January 2025

Written by: Brandon Butler, Senior Research Analyst, Enterprise Networks

Introduction

The advent of the AI era is fundamentally changing how enterprises approach their IT strategy, including for their networks. IDC survey data shows the optimism end users have in using AI for transforming their networking strategies, engineering, and operations (see Key Stats). However, taking advantage of the AI opportunity in networking comes with challenges, from the complexity of existing systems and processes to incorporating advanced technologies.

IDC has identified a handful of key recommendations for how organizations can maximize the value of AI-powered networking. Key points to consider include platform-based approaches to AI-powered networking, focusing on the native AI capabilities of the platform, and ensuring integrated security capabilities of the full-stack platform.

Meanwhile, a software-defined wide area network (SD-WAN) remains a critically important part of full-stack networking platforms. Organizations leverage SD-WAN to optimize cloud connectivity and user experiences as well as build next-generation secure access service edge (SASE) architectures. Full-stack platform–based approaches that stretch across multiple domains of the network — from campus and branch to datacenter and cloud — with native AI and integrated security can be important aspects of an organization's network transformation strategies.

AT A GLANCE

KEY STATS

Key findings on the use of AI in networking are as follows:

- **83%** of business executives expect AI to bolster network support for digital business initiatives.
- **79%** of respondents agree or strongly agree with the following statement: "My efforts in network automation must be fueled by AI capabilities."
- **78%** of respondents agree or strongly agree that AI capabilities should heighten the productivity and value of networking staff.

(Source: IDC's *AI in Networking Special Report Survey,* July 2024; n = 1,209)

AI-Powered Network Management

Fundamentally, AI-powered networking could transform how organizations deploy, manage, optimize, and fix networks. Two simultaneous factors are converging to create more advanced AI-powered network management. For one, network management tools and solutions from vendors are increasingly leveraging AI capabilities natively, building the AI tooling and models directly into the system. In this sense, organizations benefit from AI-powered network management without having to deploy or manage it themselves. Second, organizations globally are becoming more comfortable with AI systems automating network management tasks.

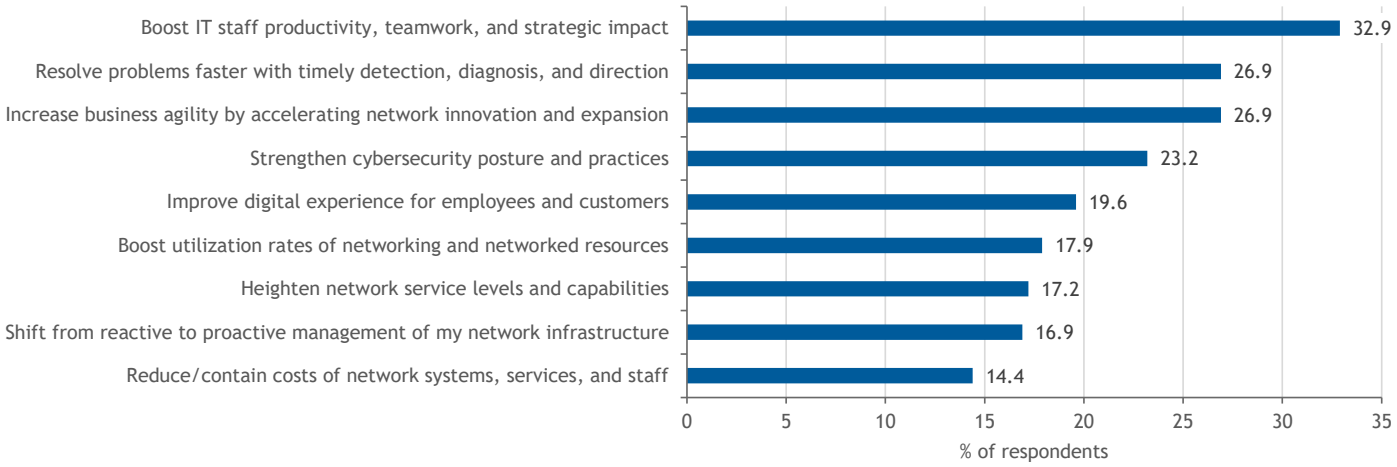
For example, IDC's July 2024 *AI in Networking Special Report Survey* asked respondents what their preferred involvement of AI-powered network automation would be. About one-third of respondents (36%) said that they would prefer an AI system to guide staff actions but not execute automated management actions. The top-rated reply by 47.5% of global respondents was for an AI system to both determine and execute automated management actions. The smallest portion of respondents (16%) reported that they would prefer not to use AI-powered network management. The results show a clear willingness among organizations to use not only AI-powered guided recommendations but also AI-powered network automation.

So what are organizations keen on using AI-powered network management for? Another question in IDC's July 2024 *AI in Networking Special Report Survey* asked what network engineering and operations functions organizations are prioritizing for AI investments. The top responses include network automation, threat detection and response, and system/service configuration and deployment. Predictive analysis modeling and problem identification/remediation were other top responses.

Successfully applying AI-enhanced management to the network requires organizations to have focused approaches and specific use cases. Survey data identifies network data collection and filtering as a critical component of AI-powered networking, along with predictive modeling analytics, current and trend performance analysis, and anomaly detection. Figure 1 shows survey data pointing to the top benefits organizations expect from utilizing AI-powered network management. Boosting staff productivity, increasing business agility, and resolving problems faster were the top responses.

FIGURE 1: ***Top Benefits of AI-Powered Network Management***

Q *What are your organization's expected top 2 benefits of using network management tools that are powered by AI capabilities?*



n = 896

Base = respondents that have domain expertise in network management

Source: IDC's AI in Networking Special Report Survey, July 2024

SD-WAN: A Critical Component of a Full-Stack Platform

SD-WAN has emerged as a key area of focus for AI-powered networking. Globally, it is a key technology for organizations looking to optimize connectivity to the cloud and AI workloads. Fundamentally, SD-WAN infrastructure helps enterprises improve their branch and remote user connectivity by providing cost savings over traditional WAN architectures and infrastructure. SD-WAN is also a vital aspect of SASE architecture. Organizations rely on SD-WAN to provide the underlying connectivity to leverage security service edge (SSE) tools and support connectivity between users and devices as well as applications and services.

SD-WAN also plays an important role in a full-stack platform–based approach to networking, which enables integrated management across SD-WAN and into wired and wireless local area networks (LANs/WLANs) as well as datacenter, cloud, and edge applications. IDC has referred to the integration of SD-WAN with LANs/WLANs as SD-Branch architectures, which enable centralized visibility, analytics, and management of the network. By combining native AI capabilities into full-stack platforms, organizations can unlock new levels of advanced automation, optimized network experiences and applications, and enhanced security.

Recommendations for Applying AI Across the Network

As organizations look to apply AI-powered networking across their networks — including for SD-WAN — IDC has a series of recommendations, including:

» **Consider network platforms:**

- Fundamentally, networking platforms are an integrated system of hardware and software that enable more integrated management across disparate network domains — for example, across campuses, branches, network security, datacenters, the cloud, and the edge. With AI enhancement, this full-stack approach to networking can increase IT and businesswide efficiency and productivity, enrich end-user experiences, enhance security, and ultimately drive new opportunities for innovation.

  IDC research shows that organizations globally are increasingly adopting platform-based approaches to enable full-stack management of their enterprise networks. About 78% of respondents to IDC's July 2024 *AI in Networking Special Report Survey* agreed or strongly agreed with the following statement: "I am moving to an AI-powered platform approach for networking." The same survey found that 64% said they prefer a platform-based approach for GenAI workloads versus best of breed.

  There are several key elements to a successful networking platform. One is to focus on simplified experiences with cross-domain workflows. Another is to have advanced data collection, filtering, modeling, and analyzing abilities across the platform's domains, including networking, security, and partner ecosystems. Networking platforms should benefit organizations across the life cycle of day 0 planning, day 1 implementation, and day "n" ongoing management.

» **Prioritize native AI capabilities:**

- A second key recommendation for leveraging AI-powered networking is to consider the native AI capabilities of a network platform. Data that fuels the AI models is foundational to AI, so from a networking perspective, network telemetry and visibility are critical for enabling advanced automation. Native AI has a range of use cases for network management, from analyzing troves of network performance and monitoring data to enabling faster identification and remediation of problems that arise in the network and — ultimately — automatically resolving issues before they impact users or applications.

  An IDC survey question asked organizations what is necessary to build a successful AI-powered networking platform. The top responses included network data collection and filtering, predictive modeling and analytics, and performance analysis.

» **Ensure integrated security:**

- The third recommendation for leveraging AI-powered networking is to focus on integrated security across the full AI-powered networking stack. In any technology buying decision, the integrated security components are a top evaluation criterion. For example, within campus and branch networking, this includes considering zero trust network access (ZTNA) approaches and network access controls (NACs)

for role-based micro-segmentation and policy enforcement. In wide area networks, integrations of SD-WAN with cloud-based secure service edge tools, such as a cloud access security broker (CASB), secure web gateway (SWG), or firewall as a service, help organizations build a SASE architecture. Network security is a foundational element of any networking platform strategy.

Profile of Juniper Networks' AI-Native Networking Platform

Juniper Networks has a suite of tools across the enterprise campus, branch, datacenter, and security domains, all of which the cloud-based Mist management system controls. These combined elements create what the company calls an AI-native networking platform that aims to simplify operations and provide service assurance.

Key components of Juniper's portfolio include a series of network and security infrastructure tools for wired and wireless LAN, location services, SD-WAN, and SASE as well as datacenter management and metro, edge, and core wide area networking. The company's Mist platform is a microservices-based, AI-enhanced management platform for campus and branch network management.

Underpinning the Mist AI system are management tools for wired and wireless LAN, SD-WAN, security, and datacenters with integrated visibility and analytics assurance capabilities. Security tools include Access Assurance, cloud-based NACs, and full-featured next-generation firewall offerings. Open API–enabled integration also allows the networking platform to integrate with other third-party IT management systems.

In early 2024, Juniper announced a new addition to the Marvis family, the Marvis Minis, a new software-based feature of the Marvis Virtual Network Assistant (VNA) that proactively simulates user experiences to validate network configurations as well as find and detect problems across the full stack. Marvis Minis identifies connectivity issues and captures the corresponding packets for forensic evidence without any users present. The company also recently enabled Marvis Application Experience Insights, which integrates Shapley data science visualizations for predictive analysis of Zoom and Teams performance and extended the Marvis VNA's natural language processing (NLP) capabilities to work in datacenter management in addition to the campus and branch capabilities previously available.

Key components of Juniper's AI-native SD-WAN offering include the following:

- **Integrated AIOps:** Marvis Virtual Network Assistant; AIOps for SD-WAN deployment, management, optimization, troubleshooting, and repair
- **Detailed visibility and analytics:** Data to feed AI algorithms stemming from network telemetry, end-user experience monitoring, and application performance, among others
- **Tunnel-free, session-oriented routing:** With adaptive encryption to improve security, enhance user experiences, and simplify operations
- **Integrated security:** ZTNA, fine-grained segmentation, centralized policy management, intrusion prevention/detection, URL filtering, and advanced threat protection

- **Juniper SD-WAN as the foundation for SASE:** Integration with Juniper SSE tools as well as third-party SSE tools, including Zscaler
- **Microservices-based cloud management:** Enables integrated management of LAN, WLAN, SD-WAN, and security from a single AI engine

Challenges

Juniper Networks is well positioned to take advantage of the AI opportunity in networking; however, it faces challenges as it looks to further engage with organizations globally. First, organizations are at varying maturity levels in their AI-powered network management maturity. Many organizations have existing disparate or heterogeneous network management tools and potentially complex integrations with other IT operations systems. Graduating to an AI-powered, full-stack network platform approach can be a multistep and multiyear process, but one that can yield significant benefits.

Customers will also be at varying comfort levels with respect to leveraging advanced, AI-powered network engineering and operations capabilities. Here, Juniper will work with customers on road map approaches such as leveraging AI-powered NLP management tools or providing optimization recommendations before implementing automated network management actions. Keys to Juniper being successful include educating customers on the specific use cases and business benefits of AI-powered networking platforms and having tools that cater to customers' maturity levels.

Conclusion

As organizations across the globe look to take advantage of the opportunities in the AI era, tremendous potential exists. The continued rapid development and adoption of AI capabilities across several domains will mean that organizations must have agile and scalable platforms. The AI networking opportunity, both "networking for AI" and "AI for networking," represents foundational and generational shifts in the networking industry.

About the Analyst

Brandon Butler, *Senior Research Manager, Enterprise Networks*

Brandon's research focuses on market and technology trends, forecasts, and competitive analysis in enterprise campus and branch networks. His coverage includes technologies used in local and wide area networking, such as Ethernet switching, routing/SD-WAN, wireless LAN, and enterprise network management platforms.

MESSAGE FROM THE SPONSOR

Juniper's AI-Native Networking Platform leverages industry-leading AIOps to deliver exceptional operator and end-user experiences across all networking domains, including wireless access, wired access, SD-WAN, WAN Edge, datacenters, and security. Powered by a common cloud and AI engine, the platform uses artificial intelligence, machine learning, and data science techniques to simplify operations and optimize network performance. With over nine years of AI learning, Juniper's platform ensures reliable, measurable, and secure connections for every device, user, and application. It reduces operational complexity, achieving up to 90% fewer trouble tickets, 85% fewer truck rolls, and 9x faster deployment.

Learn more about how Juniper delivers a simplified experience for those who run networks and those who depend on them at Juniper.net.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

140 Kendrick Street

Building B

Needham, MA 02494, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

blogs.idc.com

www.idc.com

2000831-001-EN Feb 2025